INDICATORS OF BEHAVIOR

Overview of Revision 2 Reference Implementation

Presentation to IOB Sub-Project Members

August 15, 2023

Charlie Frick, Johns Hopkins Applied Physics Lab,
Charles.Frick@jhuapl.edu

Acknowledgement:
Contributions from Dr. Vasileios Mavroeidis, University of Oslo, OASIS CACAO Project

Overview

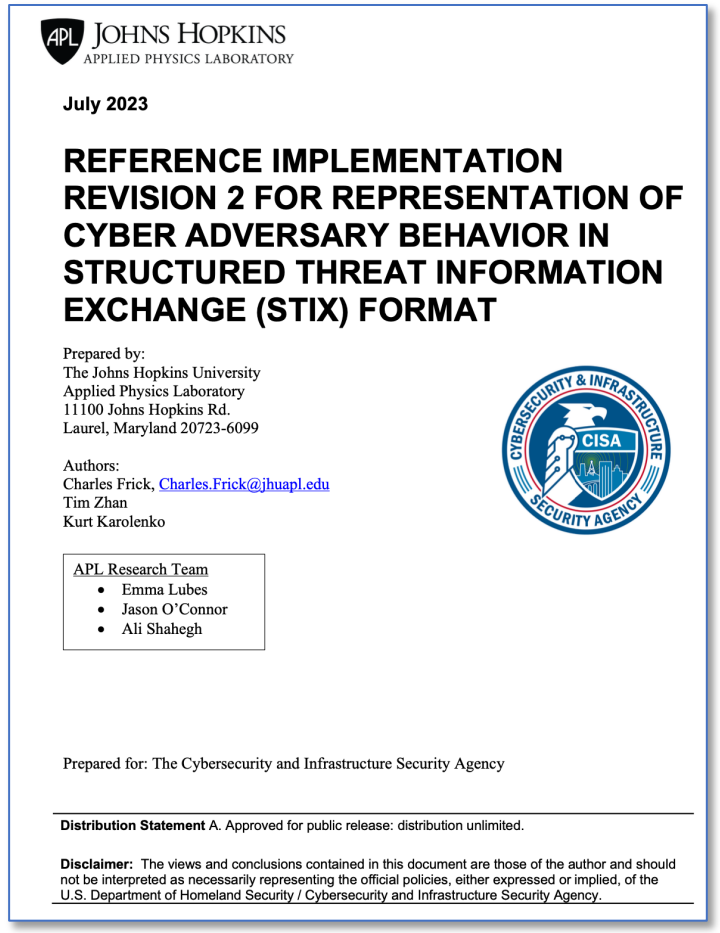
- Johns Hopkins Applied Physics Lab released revision 2 of the IOB reference implementation in July 2023
  - Available at https://github.com/opencybersecurityalliance/oca-iob/tree/main/apl_reference_implementation_bundle/revision_2

- This presentation will provide an overview of the new features which have incorporated your feedback provided in the IOB Sub-Project meetings. Thank you for your contributions.

Access the Reference Implementation on GitHub

Documentation

- Update on GitHub repository also includes updated technical documentation with full explanation of IOB features and examples for IOB use



JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

July 2023

REFERENCE IMPLEMENTATION REVISION 2 FOR REPRESENTATION OF CYBER ADVERSARY BEHAVIOR IN STRUCTURED THREAT INFORMATION EXCHANGE (STIX) FORMAT

Prepared by:
The Johns Hopkins University
Applied Physics Laboratory
11100 Johns Hopkins Rd.
Laurel, Maryland 20723-6099

Authors:
Charles Frick, Charles.Frick@jhuapl.edu
Tim Zhan
Kurt Karolenko

APL Research Team
- Emma Lubes
- Jason O'Connor
- Ali Shahegh

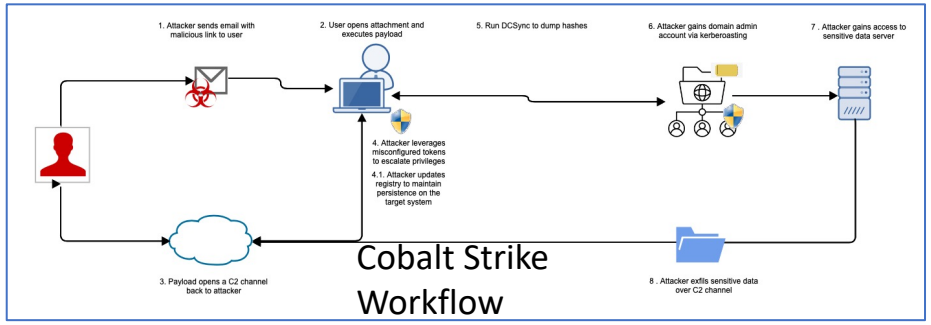
Prepared for: The Cybersecurity and Infrastructure Security Agency

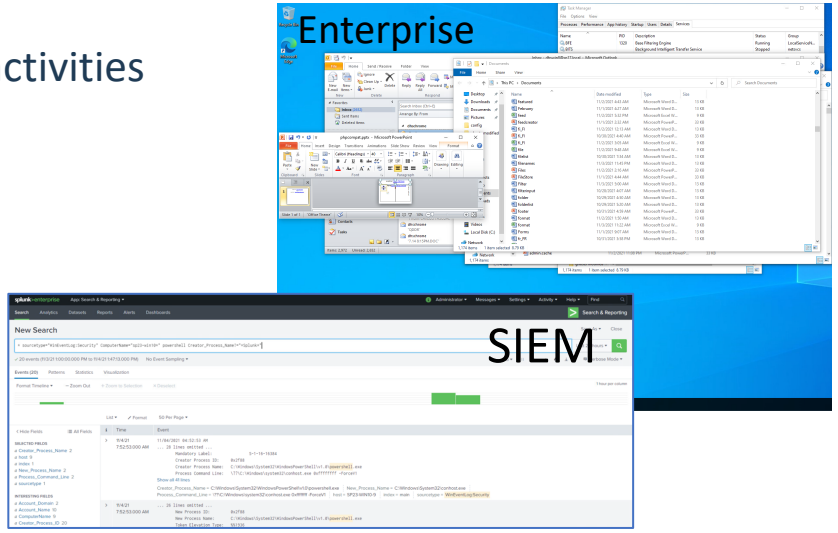
Distribution Statement A. Approved for public release: distribution unlimited.

Disclaimer: The views and conclusions contained in this document are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security / Cybersecurity and Infrastructure Security Agency.

Current Reference Prototype

- A 3000+ line JSON STIX bundle compliant with STIX 2.1 spec
- Represents observed behaviors from an emulated attack based on APT 37 / “Reaper”
- Includes behaviors and detections in shareable Sigma rule format
  - Detections tested against emulated enterprise network with a SIEM, endpoint, and network sensors
  - Enterprise machines conduct general user activities so analytic false positives can be reduced





To exercise this new approach, we have created and tested a bundle for an example APT attack

STIX2NEO4J Script

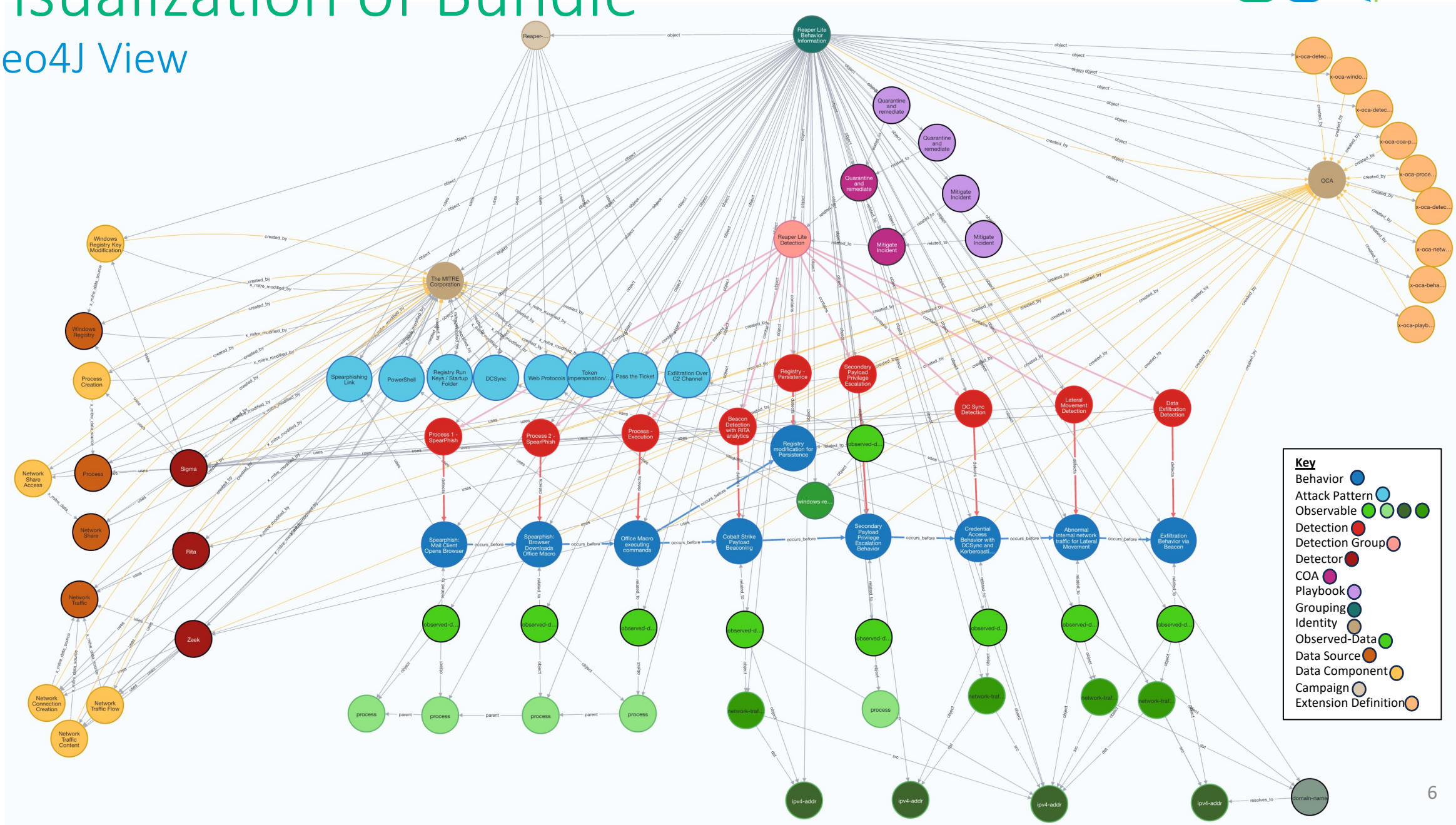
- Python script for analyzing STIX 2.x bundles in a neo4j graph database
- Provides additional analytical capabilities for investigating raw STIX messages without major modification of the data
  - Threat Intel Platforms often make significant changes to data model upon import
- Released on an Apache2 license through the Open Cybersecurity Alliance Indicator of Behavior Sub-Project
- Script repository link on GitHub:
  - https://github.com/opencybersecurityalliance/oca-iob/tree/main/STIX2NEO4J%20Converter

SCAN ME

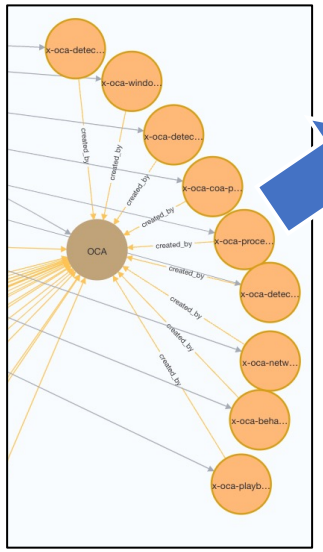
INDICATORS OF BEHAVIOR

Visualization of Bundle

Neo4J View



Visualization of Bundle – Extensions



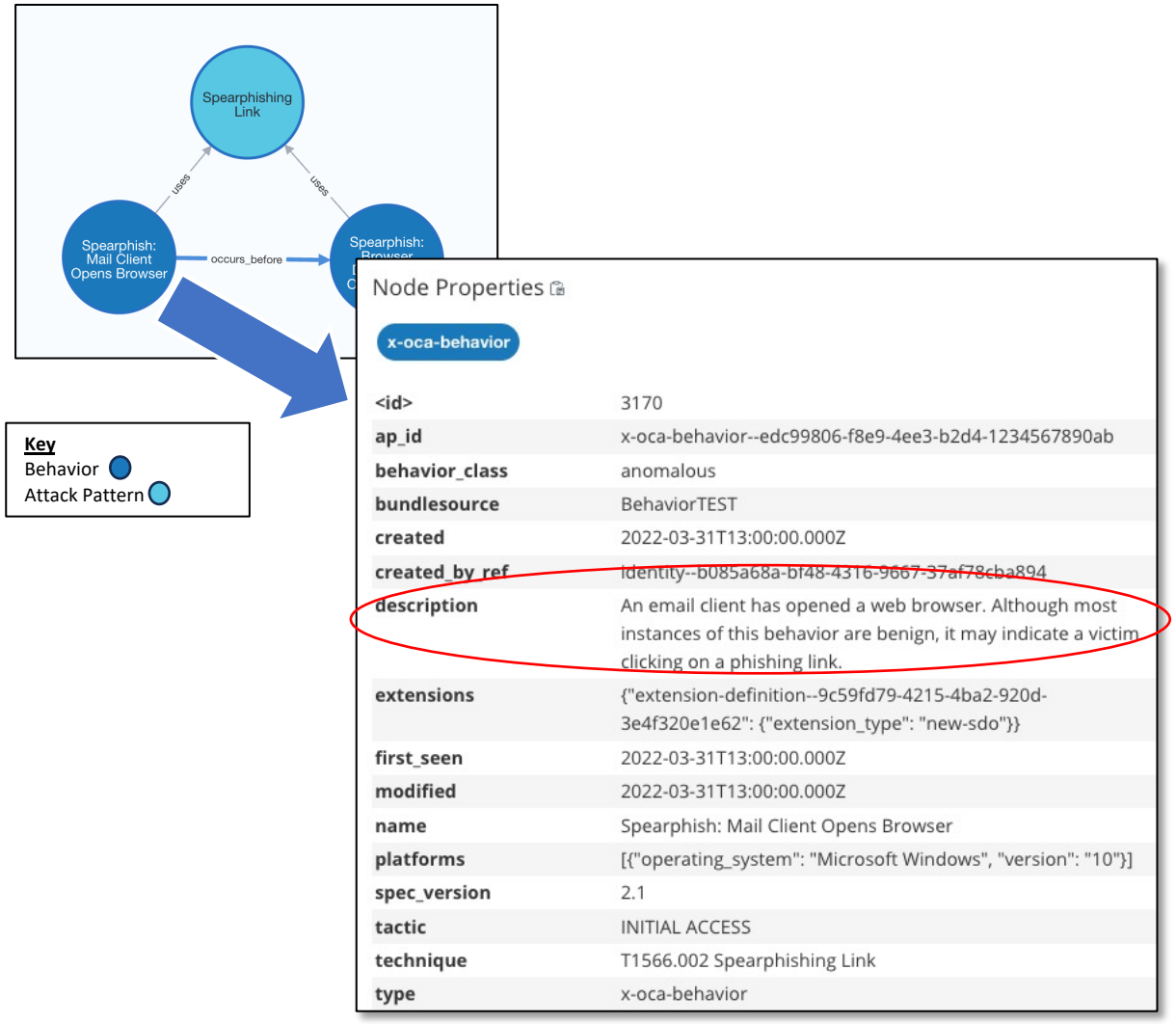
Key
Extension Definition
Identity

extension-definition

<id>	3304
ap_id	extension-definition--2cf8c8c2-69f5-40f7-aa34-efcef2b912b1
bundlesource	BehaviorRev2
created	2022-03-31T13:00:00.000Z
created_by_ref	identity--b085a68a-bf48-4316-9667-37af78cba894
description	This schema extends the Windows Registry Key SCO.
extension_types	["property-extension"]
modified	2022-03-31T13:00:00.000Z
name	x-oca-windows-registry-key Extension Definition
schema	https://raw.githubusercontent.com/opencybersecurityalliance/oca-iob/main/apl_reference_implementation_bundle/revision_2/schemas/observables/extended-windows-registry-key.json
spec_version	2.1
type	extension-definition
version	1.0.0

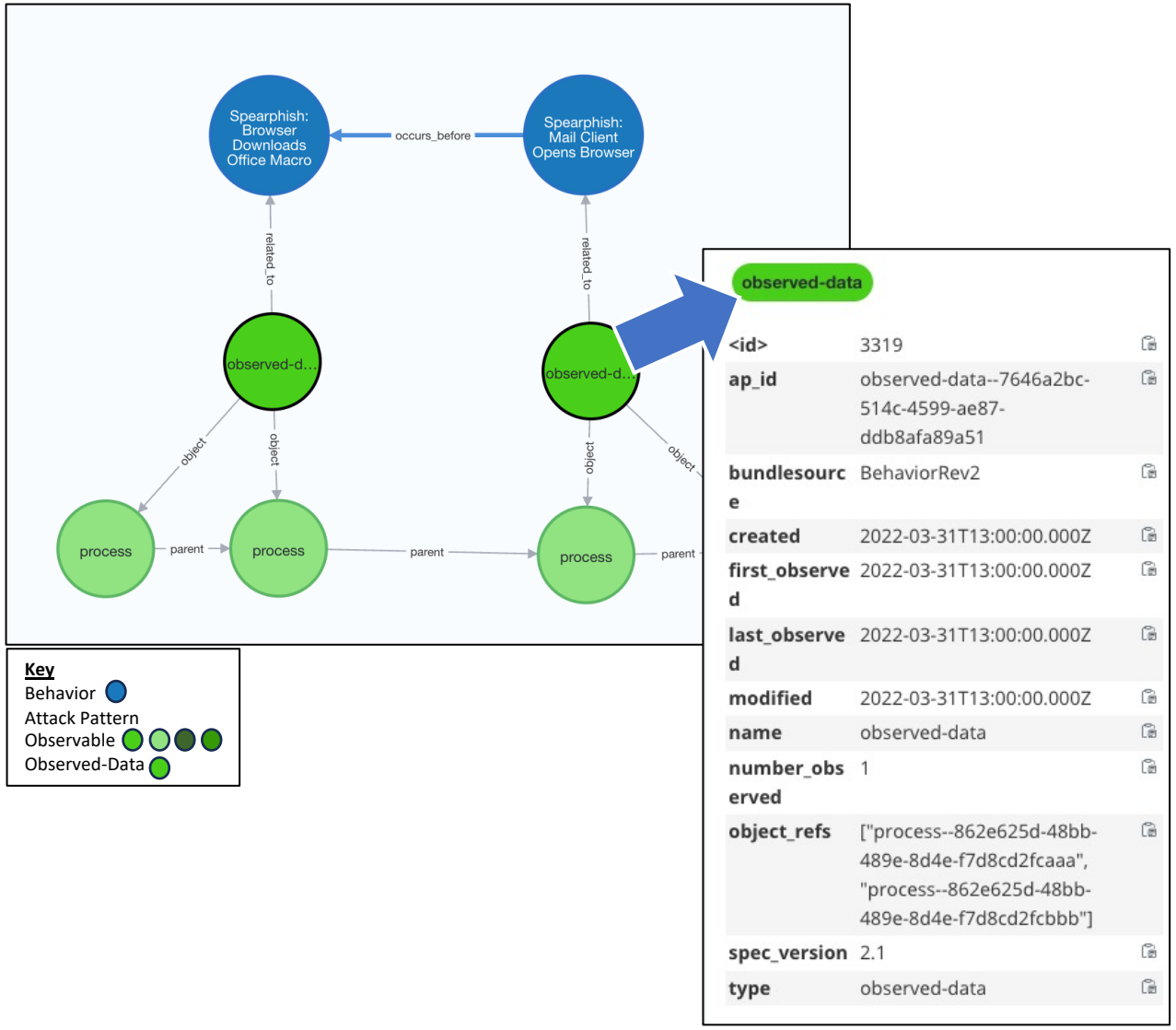
- IOB use of STIX requires multiple extensions
- Revision 2 includes all extension definitions
- Associated with OCA Identity objects
- Reference implementation now includes valid links to all extension JSON schema as well
- Currently coordinating efforts across all OCA to include common STIX extensions on GitHub

Visualization of Bundle – Behavior Object



- Each Behavior Object summarizes one of the behavior steps in the overall sequence
- Object metadata contains links to relevant MITRE ATT&CK entries
  - Multiple behaviors and behavior sets could map to these ATT&CK techniques
- As will be seen on the following slides, multiple node types will link to the Behavior Object node to define the overall behavior
  - Observables
  - Detection analytics
- Multiple Behavior Objects are linked together to represent the overall sequence of the behavior set

Visualization of Bundle – Observed Data

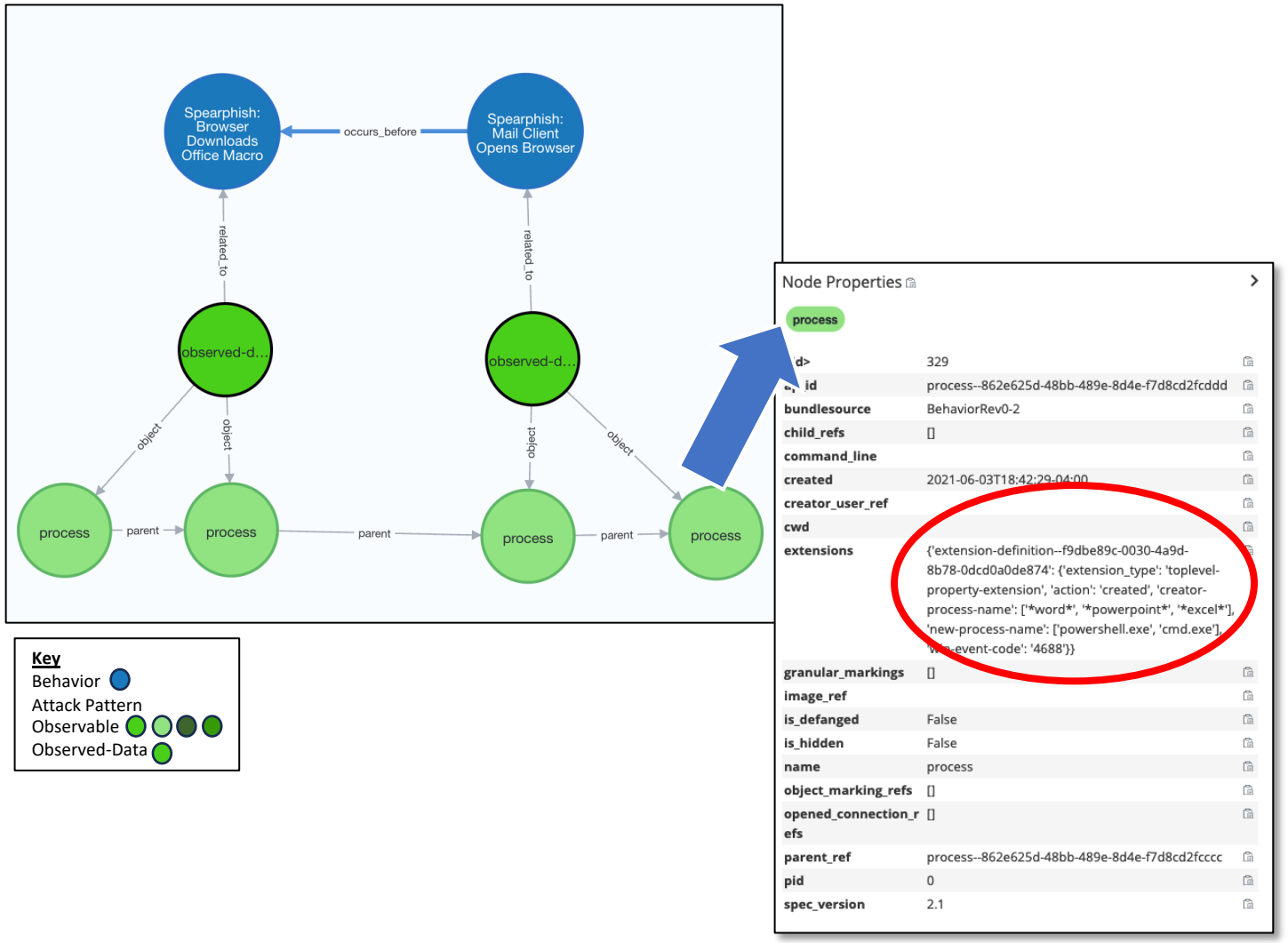


observed-data

<id>	3319
ap_id	observed-data--7646a2bc-514c-4599-ae87-ddb8afa89a51
bundlesource	BehaviorRev2
created	2022-03-31T13:00:00.000Z
first_observed	2022-03-31T13:00:00.000Z
last_observed	2022-03-31T13:00:00.000Z
modified	2022-03-31T13:00:00.000Z
name	observed-data
number_observed	1
object_refs	["process--862e625d-48bb-489e-8d4e-f7d8cd2fcaaa", "process--862e625d-48bb-489e-8d4e-f7d8cd2fcbbb"]
spec_version	2.1
type	observed-data

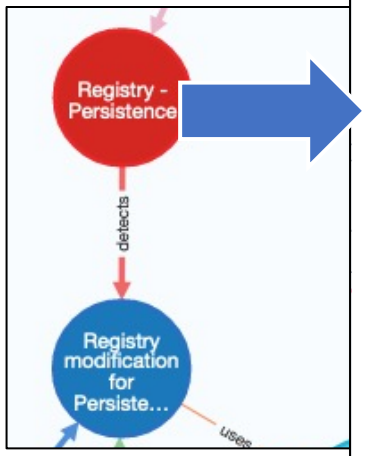
- Previous comments from IOB Project members were concerned about support for stix-patterning with respect to observables
- To address these concerns, revision 2 includes STIX “observed-data” objects to better support patterning
- Note: the observations in an IOB bundle are more for justification to explain the detections. It is recommended to use the detection objects and include STIX-Shifter detections if one wishes to detect behavior with patterns.

Visualization of Bundle – Observables



- Our spearphishing behavior also includes relationships to a chain of Process STIX Cyber Observables
- Process metadata includes information on data sources to search for the process
- Also defines which process calls it
- Highlighted example is a common process for searching/correlating 2 behaviors in the set

Visualization of Bundle – Detection



Key
Behavior
Detection

Node Properties

x-oca-detection

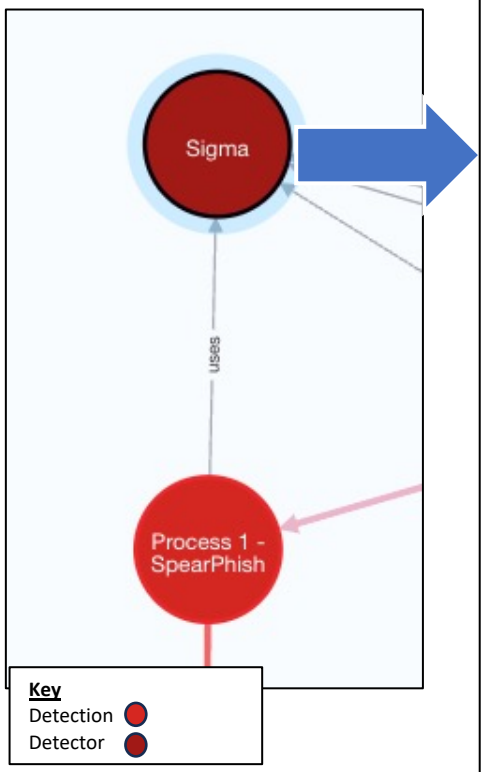
<id>	3220
analytic	{"rule": LS0tCnRpdGxlOiBSZWdpc3RyeSBSdW4gS2V5cwppZDog...aXN0cnkgcGVyc2lzdGVuY2UKc3RhdHVzOiBleHBlcmltZW50YWwKZGVzY3JpcHRpb246IERldGVjdHMgbmV3IHJlZ2lzdHJ5IHJ1biBkZXkgY3JlYXRlZCBldmVudC4KdGFnczoKLSBhdHRhY2suc3VicGVyc2lzdGVuY2UKLSBhdHRhY2sudDE1NDcKYXV0aG9yOiBkZW1vCmRhdGU6IDIwMjEvMDYvMDcKbG9nc291cmNlOgogIHByb2R1Y3Q6IHdpbmRvd3MKICBpbmRleDogbWFpbgogIGNhdGVnb3J5OiBByZWdpc3RyeV9ldmVudApkZXRlY3Rpb246CiAgc2VsZWN0aW9uOgogICAgRXZlbnRDb2RlOiAnNDY1NycKICAgIE9iamVjdF9OYW1lfGNvbnRhaW5zOgogICAgLSBSdW4KICAgIC0gU2hlbGwgRm9sZGVycwogIGNvbmRpdGlvbjogc2VsZWN0aW9uCmZhbHNlcG9zaXRpdmVzOgotIEhpZ2gKbGV2ZWw6IGhpZ2g=", "type": "Sigma Rule - base64 encoded YAML file"}
ap_id	x-oca-detection--458c02c9-3635-42e4-8873-67[illegible]00517e7
bundlesource	BehaviorTEST
created	2022-03-31T13:00:00.000Z
created_by_ref	identity--b085a68a-bf48-4316-9667-37af78cba894
data_sources	[{"EventCode": "4657", "LogName": "Security", "Message": "A registry value was modified.\n\nSubject:\n\tSecurity ID:\t\tS-1-5-21-1102256457-2379380313-1247321256-500\n\tAccount Name:\t\tAdministrator\n\tAccount Domain:\t\tSP17\n\tLogon ID:\t\t0x1A1ADFE8\n\nObject:\n\tObject Name:\t\t\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\n\tObject Value Name:\tpersist\n\tHandle ID:\t\t0x918\n\tOperation Type:\t\tNew registry value created\n\nProcess Information:\n\tProcess ID:\t\t0x18f0\n\tProcess Name:\t\tC:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\n\nChange Information:\n\tOld Value Type:\t\t-\n\tOld Value:\t\t-\n\tNew Value Type:\t\tREG_SZ\n\tNew Value:\t\tTrue", "TaskCategory": "Registry", "data_type": "WinEventLog:Security"}]
extensions	{"extension-definition--c4690e13-107e-4796-8158-0dcf1ae7bc89": {"extension_type": "new-sdo"}}
modified	2022-03-31T13:00:00.000Z
name	Registry - Persistence
spec_version	2.1
type	x-oca-detection

Decoded

```
---
title: Registry Run Keys
id: registry persistence
status: experimental
description: Detects new
registry run key created event.
tags:
- attack.persistence
- attack.t1547
author: demo
date: 2021/06/07
logsource:
  product: windows
  index: main
  category: registry_event
detection:
  selection:
    EventCode: '4657'
    Object_Name|contains:
    - Run
    - Shell Folders
  condition: selection
falsepositives:
- High
level: high
```

- The information in the STIX Cyber Observables allow us to create a shareable detection analytic linked to the behavior
- Highlighted example shows a detection for web browser downloading and opening a macro-enabled MS Office file in Sigma rule format
- Rule is stored as base64 string to preserve formatting

Visualization of Bundle – Detector



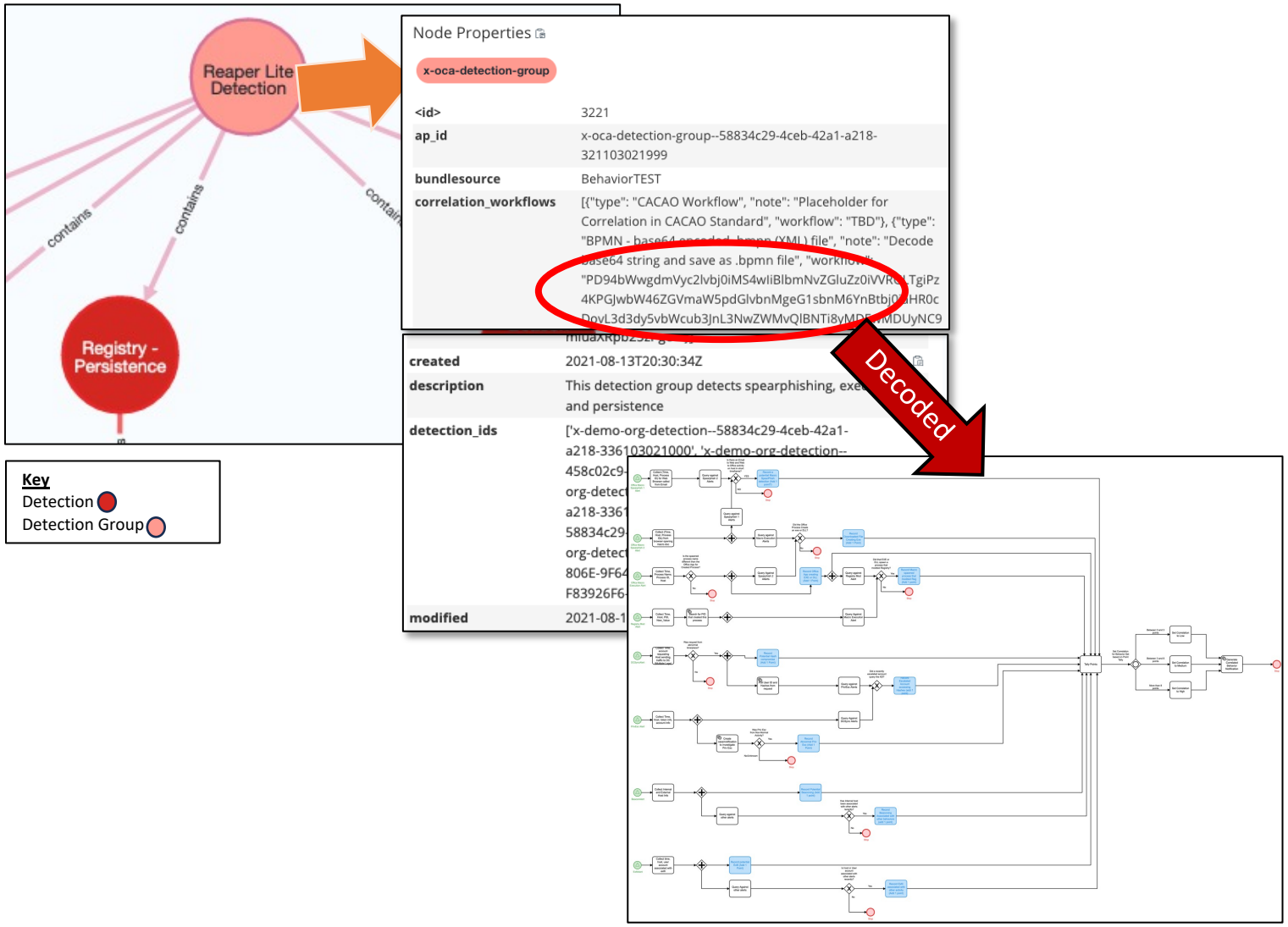
Node Properties

x-oca-detector

<id>	3174
ap_id	x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e
bundlesource	BehaviorTEST
cpe	cpe:2.3:a:sigmahq:sigma:0.21:*:*:*:*:*:*:*
created	2023-05-01T12:00:00.000Z
created_by_ref	identity--b085a68a-bf48-4316-9667-37af78cba894
description	A generic signature format for log files.
detection_types	["log"]
detector_data_categories	["log"]
detector_data_sources	["windows event log", "sysmon", "zeek", "rita"]
extensions	{"extension-definition--5cccba5c-0be4-450c-8672-b66e98515754": {"extension_type": "new-sdo"}}
modified	2023-05-01T12:00:00.000Z
name	Sigma
product	Sigma
product_url	https://github.com/SigmaHQ/sigma
product_version	0.21
spec_version	2.1
type	x-oca-detector
valid_until	2027-05-01T12:00:00.000Z
vendor	SigmaHQ
vendor_url	https://github.com/SigmaHQ

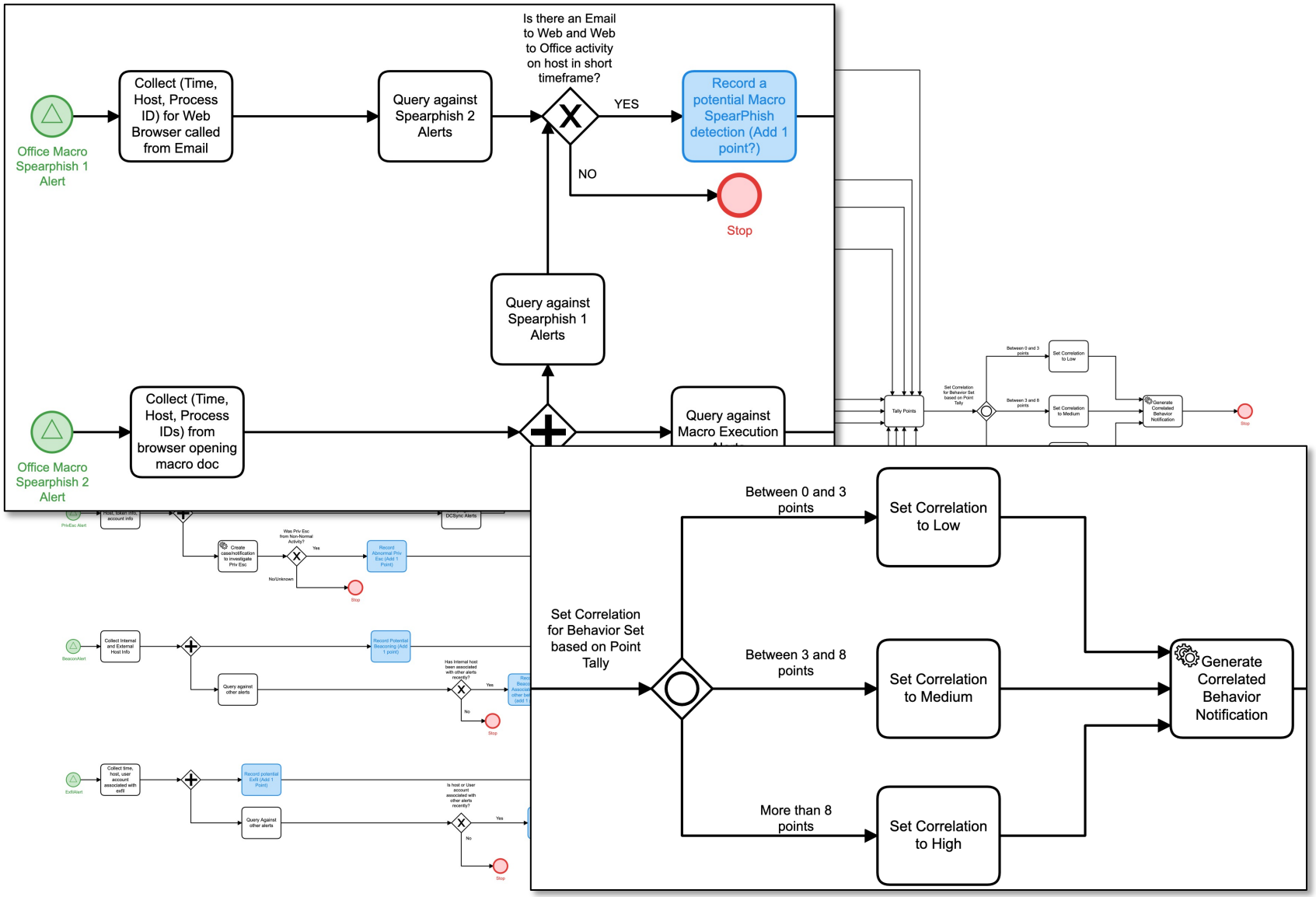
- Each detection contains relationships to the detector(s) used for detection
- Includes description and access information for sensor/tool
- Allows receivers to understand what is needed for this rule to function

Visualization of Bundle – Detection Group



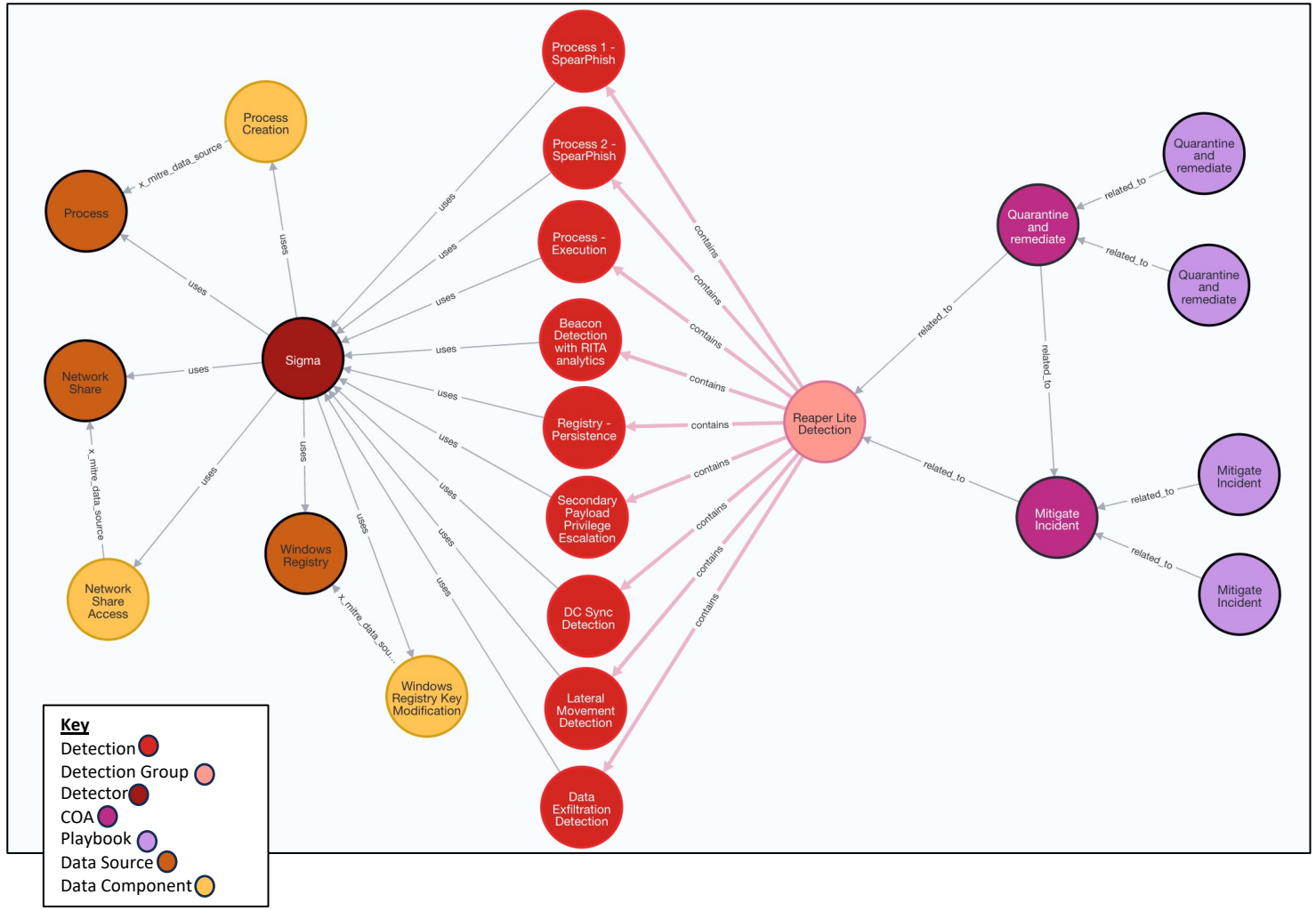
- Any single detection analytic within the bundle is prone to false positives
- The Detection Group Object exists in the bundle to help correlate the detections and explain which fields should be common between queries
- Includes base64 encoded Business Process Model Notation (BPMN) for visual and planned support for Collaborative Automated Course of Action Operations (CACAO) standard workflow

Sample Detection Group Correlation Workflow



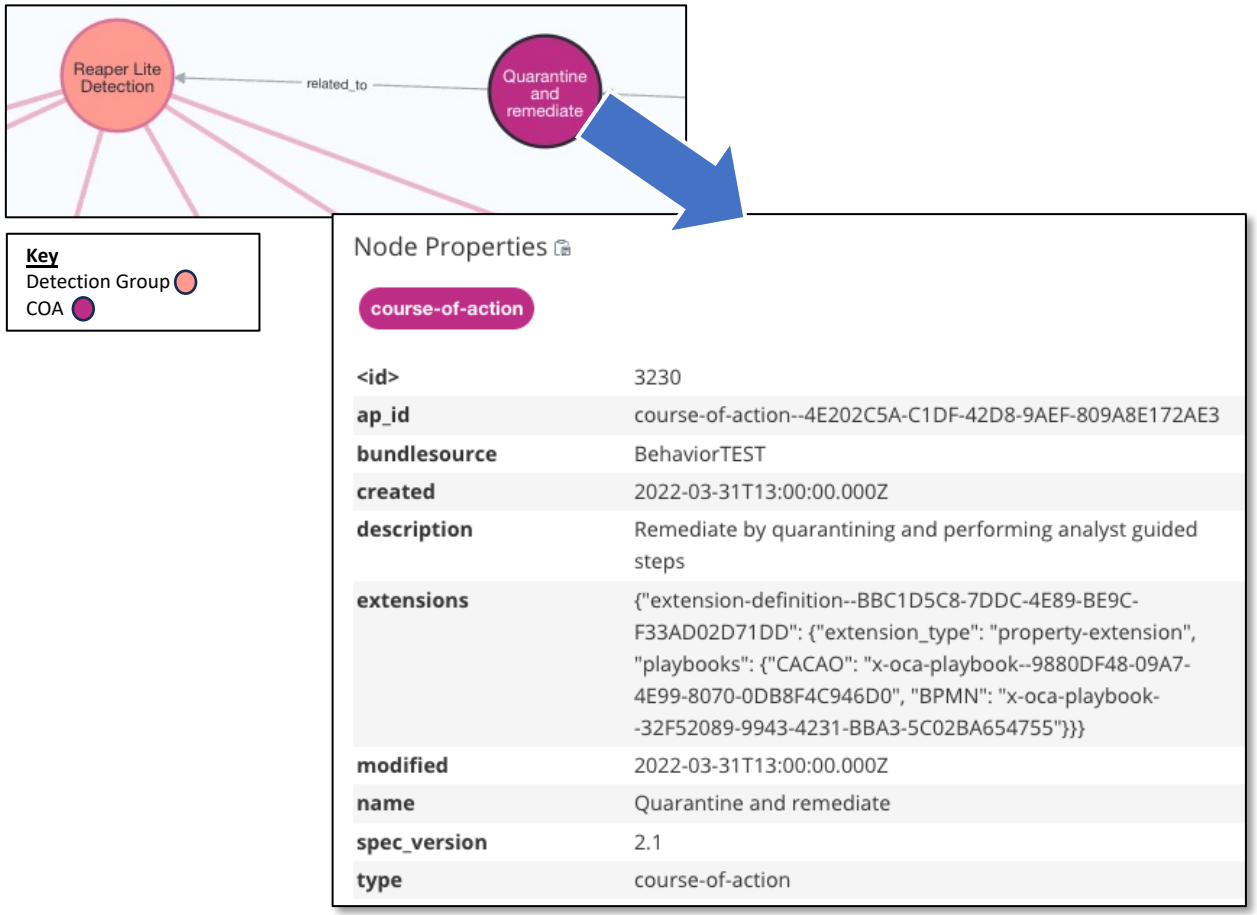
- Provides logic for how to correlate alerts from the set of detections shared in the bundle
- Any single alert may have multiple false positives
- Correlated alerts allow for higher fidelity of detections
- Can be run with automation or manually

Additional Data to support Detectors and Detections



- IOB is designed with support for automation
- Sharing detector information will require sharing the data types required
- IOB integrated Data Source, Data Component objects from MITRE ATT&CK to support this need
- The sequence of detections can be correlated in the Detection Group, leading to recommended Courses of Action and Playbooks

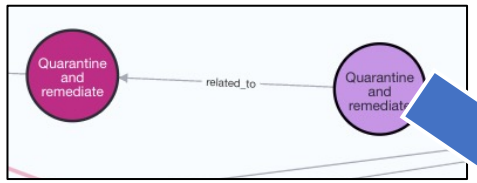
Visualization of Bundle – COA



<id>	3230
ap_id	course-of-action--4E202C5A-C1DF-42D8-9AEF-809A8E172AE3
bundlesource	BehaviorTEST
created	2022-03-31T13:00:00.000Z
description	Remediate by quarantining and performing analyst guided steps
extensions	{"extension-definition--BBC1D5C8-7DDC-4E89-BE9C-F33AD02D71DD": {"extension_type": "property-extension", "playbooks": {"CACAO": "x-oca-playbook--9880DF48-09A7-4E99-8070-0DB8F4C946D0", "BPMN": "x-oca-playbook--32F52089-9943-4231-BBA3-5C02BA654755"}}}
modified	2022-03-31T13:00:00.000Z
name	Quarantine and remediate
spec_version	2.1
type	course-of-action

- Once a correlated set of detections is identified, IOB bundles also can share Courses of Action (COA)
- Extension identifies information on multiple playbooks that can achieve the COA

Visualization of Bundle – Playbooks



Key
COA
Playbook

Node Properties

x-oca-playbook

<id>	3228
ap_id	x-oca-playbook--9880DF48-09A7-4E99-8070-0DB8F4C946D0
bundlesource	BehaviorTEST
created	2022-03-31T13:00:00.000Z
description	Remediate by quarantining and performing analyst guided steps. Optionally checks configuration management and attempts to automatically rebuild if necessary.
extensions	{"extension-definition--809C4D84-7A6E-4039-97B4-DA9FEA03FCF9": {"extension_type": "new-sdo"}}
modified	2022-03-31T13:00:00.000Z
name	Quarantine and remediate
playbook_abstraction	template
playbook_bin	ewog[illegible]

Decoded

CACAO Playbook


```
{
  "type": "playbook",
  "spec_version": "1.0",
  "id": "playbook--767d859e-7387-4e0c-95c0-458ca369486f",
  "name": "Process_1811f8w: Quarantine and Remediate",
  "description": "",
  "playbook_types": [ "mitigation", "remediation" ],
  "created_by": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "workflow_start": "start--ece532df-970a-417c-a125-5e7713e10f7c",
  "workflow": {
    "start--ece532df-970a-417c-a125-5e7713e10f7c": {
      "type": "start",
      "name": "StartEvent_1: System Course of Action Alert",
      "on_completion": "single--d22408fc-a99c-4c45-8770-27dac6df293a"
    },
    "end--4d3134d9-68d2-4bde-87ca-a5bfe8468aa6": {
      "type": "end",
      "name": "Event_17zpsn5: End"
    },
    "single--d22408fc-a99c-4c45-8770-27dac6df293a": {
      "type": "single",
      "name": "Activity_1vv8yyz: Quarantine system",
      "commands": [{
        "type": "http-api"
      }],
      "on_completion": "single--d1d15ab7-b557-4f82-8d9b-495438a5c9a9"
    },
    "single--d1d15ab7-b557-4f82-8d9b-495438a5c9a9": {
      "type": "single",
      "name": "Activity_0i91gen: Create ticket",
      "commands": [{
        "type": "http-api"
      }],
      "on_completion": "single--3efbe056-6d1e-4407-89bb-bb54016d9dea"
    },
    "single--3efbe056-6d1e-4407-89bb-bb54016d9dea": {
      "type": "single",
      "name": "Activity_1jfyg0y: Comment in ticket that system is quarantined",
      "commands": [{
        "type": "http-api"
      }],
      "on_completion": "single--27f8278c-8b87-4815-8f40-9c6af610203e"
    },
    "single--fec56d3d-47a4-4f4b-a0a7-eb42698c1e8b": {
      "type": "single",
      "name": "Activity_0uvmcne: Remove quarantine from system",
      "commands": [{
        "type": "http-api"
      }],
      "on_completion": "single--3f0e83da-5c37-4816-9d8e-7f55ef4b77a4"
    },
    "single--3f0e83da-5c37-4816-9d8e-7f55ef4b77a4": {
      "type": "single",
      "name": "Activity_1ufu0ds: Comment in ticket that system is restored and
the quarantine is removed",
      "commands": [{
        "type": "http-api"
      }],
      "on_completion": "single--b7918134-3807-4432-b47e-8a4fef268035"
    },
    "single--b7918134-3807-4432-b47e-8a4fef268035": {
      "type": "single",
      "name": "Activity_07vriey: Close ticket",
      "commands": [{
        "type": "http-api"
      }],
      "on_completion": "end--4d3134d9-68d2-4bde-87ca-a5bfe8468aa6"
    },
    "single--73fcbed4-393b-4bcd-88e2-69314c8e827c": {
      "type": "single",
      "name": "Activity_152668n: SOC analyst restores affected system",
      "commands": [{
        "type": "manual"
      }],
      "on_completion": "single--fec56d3d-47a4-4f4b-a0a7-eb42698c1e8b"
    },
    "single--27f8278c-8b87-4815-8f40-9c6af610203e": {
      "type": "single",
      "name": "Activity_12ln1os: Send email to SOC analyst to review ticket",
      "commands": [{
        "type": "http-api"
      }],
      "on_completion": "single--73fcbed4-393b-4bcd-88e2-69314c8e827c"
    }
  }
}
```


- COA objects can contain relationships to multiple shared playbook formats to achieve the COA
- Base64 encoded string decodes to playbooks in specified formats (e.g. CACAO standard format)

Conclusion

- Revision 2 would not have been possible without the contributions of our Sub-Project's community. Thank you for your help.

- As we move forward, we will continue to incorporate your feedback and focus on adoption efforts throughout the OCA and larger cyber community

- For more information:
  - IOB Project page: https://opencybersecurityalliance.org/iob/
  - IOB GitHub for documentation, use cases, reference implementation https://github.com/opencybersecurityalliance/oca-iob